

Your Ref: 217.1008.03  
Our Ref: 198147

**Request for National Phase Entry of  
an International Application**

**1. International Application No.:**

**PCT/US03/21650**

**2. Title of the Invention:**

**SECURE PRESENTATION OF ENCRYPTED DIGITAL CONTENT**

**3. International Filing Date:**

**July 9, 2003**

**4. Inventor(s):**

**MALCOLM, Michael, A.  
COLLENS, Daniel, A.  
WATSON, Stephen  
RECHSTEINER, Paul  
HUI, Kevin**

**5. Applicant(s):**

**KALEIDESCAPE, INC.**

**6. Filing Date (National Phase Entry):**

**January 11, 2005**

【書類名】 国内書面  
【整理番号】 198147  
【提出日】 平成17年 1月11日  
【あて先】 特許庁長官殿  
【出願の表示】  
【国際出願番号】 PCT/US03/21650  
【出願の区分】 特許  
【発明者】  
【住所又は居所】 アメリカ合衆国 8 1 6 1 2 コロラド州アスペン、ポスト・オフィス・ボックス 7 6 6 7  
【氏名】 マイケル・エイ・マルコム  
【発明者】  
【住所又は居所】 カナダ、エヌ 2 ケイ・3 ゼット 8、オンタリオ、ウォータールー、ボナビスタ・ドライブ 7 9 0 番  
【氏名】 ダニエル・エイ・コレンズ  
【発明者】  
【住所又は居所】 カナダ、エム 6 ジー・2 ワイ 4、オンタリオ、トロント、クリントン・ストリート 6 5 番  
【氏名】 スティーブン・ワトソン  
【発明者】  
【住所又は居所】 カナダ、エム 5 エイ・4 ピー 7、オンタリオ、トロント、アパートメント 6 2 7、フロント・ストリート・イースト 1 0 9 番  
【氏名】 ポール・レヒスタイナー  
【発明者】  
【住所又は居所】 カナダ、エヌ 2 エム・5 イー 4、オンタリオ、キッチェナー、ウエスト・アベニュー 3 0 8 - 2 9 番  
【氏名】 ケビン・ファイ  
【特許出願人】  
【住所又は居所】 アメリカ合衆国 9 4 0 4 3 カリフォルニア州マウンテン・ビュー、スウィート 1 0 0、ノース・バーナード・アベニュー 3 3 9 番  
【氏名又は名称】 カレイドスケープ・インコーポレイテッド  
【氏名又は名称原語表記】 K A L E I D E S C A P E, I N C.  
【国籍】 アメリカ合衆国  
【代理人】  
【識別番号】 100086405  
【弁理士】  
【氏名又は名称】 河宮 治  
【電話番号】 06-6949-1261  
【ファクシミリ番号】 06-6949-0361  
【連絡先】 担当  
【選任した代理人】  
【識別番号】 100098280  
【弁理士】  
【氏名又は名称】 石野 正弘  
【電話番号】 06-6949-1261  
【ファクシミリ番号】 06-6949-0361  
【手数料の表示】  
【予納台帳番号】 163028  
【納付金額】 21,000円

【書類名】 国際出願翻訳文提出書

【整理番号】 198147

【提出日】 平成17年 3月 9日

【あて先】 特許庁長官殿

【出願の表示】

【国際出願番号】 PCT/US03/21650

【出願の区分】 特許

【特許出願人】

【識別番号】 505013158

【氏名又は名称】 カレイドスケイプ・インコーポレイテッド

【代理人】

【識別番号】 100086405

【弁理士】

【氏名又は名称】 河宮 治

【電話番号】 06-6949-1261

【ファクシミリ番号】 06-6949-0361

【提出物件の目録】

【物件名】 請求の範囲の翻訳文 1

【物件名】 明細書の翻訳文 1

【物件名】 図面の翻訳文 1

【物件名】 要約書の翻訳文 1

**【書類名】特許請求の範囲****【請求項 1】**

メディアストリームを、そのメディアストリームを表わすデジタルコンテンツフォーマットへ符号化するステップと、

そのメディアストリームを表わすデジタルコンテンツフォーマット全体より少ない、そのデジタルコンテンツの一部分を暗号化するステップであって、暗号化されたデジタルコンテンツの一部分は、メディアストリームの提示に必要である、ステップと

を含み、そのデジタルコンテンツの暗号化されたバージョンは、フォーマットパラメータにおいて、そのデジタルコンテンツの暗号化されていないバージョンから実質的に変化していない、方法。

**【請求項 2】**

前記符号化ステップが、少なくとも若干のビデオデータの M P E G 符号化を提供する、請求項 1 に記載の方法。

**【請求項 3】**

前記暗号化ステップが、ブロック換字暗号を用いて、少なくとも若干のオーディオデータあるいはビデオデータを暗号化するステップを含んでいる、請求項 1 に記載の方法。

**【請求項 4】**

前記暗号化ステップは、

ブロック換字暗号を用いて、少なくとも若干のオーディオあるいはビデオデータを暗号化するステップと、

そのブロック換字暗号を用いて、少なくとも若干のオーディオあるいはビデオデータを暗号化することを抑えるステップであって、ここで、暗号化されていないオーディオあるいはビデオデータの量が、ブロック換字暗号のためのブロックサイズより少ないステップと

を含む、請求項 1 に記載の方法。

**【請求項 5】**

前記暗号化ステップは、

デジタルフォーマット内の少なくとも第 1 組のデータおよび第 2 組のデータを識別するステップと、

第 1 組のデータおよび第 2 組のデータを別々に暗号化するステップとを含み、

それにより、第 1 組のデータは第 1 組のユーザに利用可能に作成することができ、第 2 組のデータは第 2 組のユーザに利用可能に作成することができ、第 1 組のユーザは、第 2 組のユーザと区別可能である、請求項 1 に記載の方法。

**【請求項 6】**

前記暗号化ステップは、

(a) 少なくとも若干のオーディオあるいはビデオデータを説明する情報、あるいは、(b) 少なくとも何らかのフォーマット情報のうちの少なくとも 1 つの暗号化を抑えるステップを含む、請求項 1 に記載の方法。

**【請求項 7】**

デジタルコンテンツのフォーマットが、少なくとも若干のオーディオあるいはビデオデータと、少なくとも何らかのフォーマット情報を含んでいる、請求項 1 に記載の方法。

**【請求項 8】**

そのメディアストリームを表わすデジタルコンテンツのフォーマットが、相対的に高レベルの各層が抽象化を表わし、それに対し、相対的に低レベルの各層がその実現を表わす 1 組の層を含んでおり、

第 1 組の相対的に高レベルの層は、そのメディアストリームに対するオーディオまたはビデオ情報を表わし、一方、第 2 組の相対的に低レベルの層は、情報がフォーマットされ、あるいは補足される技術を表わしており、

暗号化のステップは、オーディオおよびビデオ情報を表わすデジタルコンテンツの部分

のみに適用される、請求項 1 に記載の方法。

【請求項 9】

そのメディアストリームを表わすデジタルコンテンツのフォーマットが、相対的に高レベルの各層が抽象化を表わし、それに対し、相対的に低レベルの各層がその実行を表わす、1 組の層を含んでおり、

第 1 組の相対的に高レベルの層は、そのメディアストリームに対するオーディオおよびビデオ情報を表わし、一方、第 2 組の相対的に低レベルの層は、情報が各パケットへ断片化され、索引をつけられ、複合化され、またはメタデータで補足される技術を表わしており、

暗号化のステップは、オーディオおよびビデオ情報を表すデジタルコンテンツの部分のみに適用される、請求項 1 に記載の方法。

【請求項 10】

そのメディアストリームを表わすデジタルコンテンツのフォーマットが、相対的に高レベルの各層が抽象化を表わし、それに対し、相対的に低レベルの各層がその実行を表わす 1 組の層を含んでおり、

第 1 組の相対的に高レベルの層は、そのメディアストリームに対するオーディオおよびビデオ情報を表し、一方、第 2 組の相対的に低レベルの層は、情報が各パケットへ断片化され、索引をつけられ、複合化されまたはメタデータで補足される技術を表しており、

暗号化のステップは、オーディオおよびビデオ情報以外を表わすデジタルコンテンツの当該部分の少なくとも一部には適用されない、請求項 1 に記載の方法。

【請求項 11】

メディアストリームが、映画、アニメーション、音、静止メディア、写真、イラスト、データベース、情報のコレクションのうちの少なくとも 1 つを含んでいる、請求項 1 に記載の方法。

【請求項 12】

そのデジタルコンテンツの配布において、実質的に全く変化がないように、暗号化するデジタルコンテンツの部分を選択するステップを含んでいる、請求項 1 に記載の方法。

【請求項 13】

前記選択ステップが、そのデジタルコンテンツ内の 1 組のデジタルデータの packets において、実質的に全く変化がないのを確実にすることを含んでいる、請求項 12 に記載の方法。

【請求項 14】

前記選択ステップが、メディアストリームのオーディオとビデオ部分との同期化において、実質的に変化がないのを確実にすることを含んでいる、請求項 12 に記載の方法。

【請求項 15】

前記選択ステップが、そのデジタルコンテンツ内の少なくとも若干の識別可能なオーディオあるいはビデオデータの長さにおいて、実質的に変化がないのを確実にすることを含んでいる、請求項 12 に記載の方法。

【請求項 16】

通信リンクへ結合可能な入力ポートであって、通信リンクは、デジタルコンテンツを担持することが可能であり、デジタルコンテンツは、少なくとも何らかの提示可能な情報および少なくとも何らかのフォーマット情報を含んでいる、入力ポートと、

フォーマット情報に対応する提示可能な情報を識別することができるデジタルコンテンツデコーダと、

キーに対応して提示可能な情報を復号化することができるデジタルコンテンツ復号化装置と

を含み、復号化装置は、デコーダより相対的に比較的高度なセキュリティで保護されている、装置。

【請求項 17】

通信リンクが、

デジタルコンテンツを担持することができるコンピュータネットワークと、

物理メディアに対応して情報を検索することができるリーダーであって、物理メディアは、デジタルコンテンツを担持することができる、リーダー、の少なくとも1つを含んでいる、請求項16に記載の装置。

【請求項18】

デコーダがMPEGデコーダを含んでいる、請求項16に記載の装置。

【請求項19】

デコーダが、第1の選択された組のハードウェアあるいはソフトウェアに含まれており、第1の選択された組は信頼され、

復号化装置およびキーが、第2の選択された組のハードウェアあるいはソフトウェアに含まれており、第2の選択された組は、第1の選択された組より相対的に信頼性が高い、請求項16に記載の装置。

【請求項20】

デコーダが提示情報にアクセスすることなく、デコーダが、1つ以上のメディアストリームについての、少なくとも何らかのメタデータを提示するフォーマット情報に応答する、請求項16に記載の装置。

【請求項21】

デコーダが提示情報にアクセスすることなく、デコーダが、  
メディアストリームに対して既知である、既知の再生機能と、  
デジタルコンテンツ内のナビゲーションと、  
デジタルコンテンツ内のコンテンツ選択と、  
提示の操作と

の機能のうち少なくとも1つを提供するフォーマット情報に応答する、請求項16に記載の装置。

【請求項22】

デジタルコンテンツが、映画、アニメーション、音、静止メディア、写真、イラスト、データベース、情報のコレクションのうちの少なくとも1つを含んでいるメディアストリームを表わす、請求項16に記載の装置。

【請求項23】

相対的に高度なセキュリティが、認証されたソフトウェアの制御の下で動作する、改ざん防止ハードウェアを含んでいる、請求項16に記載の装置。

【請求項24】

デジタルコンテンツが第1メディアストリームおよび第2メディアストリームを提示し

、デコーダがフォーマット情報に反応し、復号化装置が選択されたキーに反応し、

選択されたキーが、選択されたユーザに第1メディアストリームおよび第2メディアストリームへの異なるアクセスを提供する、請求項16に記載の装置。

【請求項25】

第1メディアストリームがオーディオ情報を含んでおり、第2メディアストリームがビデオ情報を含んでおり、

第1メディアストリームが第1言語での情報を含んでおり、第2メディアストリームが第2言語での情報を含んでおり、

第1メディアストリームが第1タイプの聴衆をターゲットにした提示情報を含んでおり、第2メディアストリームが第1タイプの聴衆をターゲットにした情報を含んでいる、請求項24に記載の装置。

【請求項26】

メディアストリームを、そのメディアストリームを表わすデジタルコンテンツフォーマットへ符号化するステップであって、そのデジタルコンテンツフォーマットが、1組の情報ノードを有しており、これらの情報ノードが少なくとも部分的順序で配置されている、ステップと、

そのデジタルコンテンツの一部分を暗号化するステップであって、暗号化された部分は、そのメディアストリームを表わすデジタルコンテンツフォーマット全体より少なく、暗号化されたデジタルコンテンツの部分は、メディアストリームの提示に必要である、ステップと

を含み、そのデジタルコンテンツの暗号化されていない部分は、実質的に部分的順序の下方に閉じられており、それにより、そのデジタルコンテンツの暗号化されていない部分は、それを復号化することを要することなくデコード可能である、方法。

【書類名】明細書

【発明の名称】暗号化されたデジタルコンテンツの安全な提示方法

【技術分野】

【0001】

本発明は、デジタルコンテンツに対応するメディアストリームの提示に関する。

【背景技術】

【0002】

例えば、映画などのメディアストリームを表わすデジタルコンテンツの配布は、いくつかの問題を受ける。1つの問題は、簡単にデジタルコンテンツの正確なコピーを作成できるため、それをする権限を有しているかいないかにかかわらず、いかなる受取人もそのコンテンツを再配付可能となることである。権限なく配布される惧れがなく、デジタルコンテンツ、特にメディアストリームを表わすデジタルコンテンツを配布可能となることは有利であろう。これは、デジタルコンテンツを、例えば、コンピュータネットワーク、あるいは、（例えば、要求に応じて、あるいは今後の要求を予測して、あるいは他の何かに応じて）エンドビューアへ配布するための他の技術など、通信リンクを用いて配布することが所望されるとき、特に有利であろう。

【0003】

1つの既知の解決策は、メディアストリームを表わすデジタルコンテンツを暗号化することで、そのデジタルコンテンツの受取人が、すぐに提示可能な（すなわち、暗号化されていない）フォーマットで、権限のない受取人に容易には再配付できなくすることである。しかしながら、暗号化された形式でデジタルコンテンツが配布されたときでさえ、それをビューアへ提示可能にするには、前もって復号化されなければならない。したがって、各映画に対して、発信者からビューアへの配布の間、その映画が暗号化されていないフォーマットで利用可能（本明細書では「クリアな状態」と呼ばれることもある）となる間、の少なくとも若干の時間がかかることになる。時には、さらに場所により、いかなる提示システムであれ、その映画がクリアな状態で利用可能であると、その映画はセキュリティアタックを受けやすい。例えば、権限のない人が、認可を受けずに、暗号化されていないフォーマットでその映画をコピーし、配布あるいは使用することもある。

【0004】

したがって、デジタルコンテンツをクリアな状態で露出することなく、そのデジタルコンテンツを、提示用のメディアストリームとして使用可能な方法（および、その実行装置）を提供することは有利となろう。しかしながら、この目標の達成に関連して若干の問題がある。

【発明の開示】

【発明が解決しようとする課題】

【0005】

・クリアな状態のデジタルコンテンツを取得するワークファクタが、単純にコピーを購入するより実質的に大きくなるよう（あるいは、権限のない調達のための、他の利用可能な技術より、少なくとも大きくなるよう）、装置が相対的に改ざん防止であることが望ましいだろう。

【0006】

・また、メディアストリームを表わすデジタルコンテンツを、装置が、できる限り少ししか露出しないことも望ましいだろう。若干の例では、メモリ内にクリアな状態でデジタルコンテンツ（あるいは、そのデジタルコンテンツを得ることができたキー）を有していることは、それ自体、実際にエンドユーザに目視されるためにスクリーン上へ提示するときだけ、内部バスにクリアな状態でデジタルコンテンツを有するより、望ましくないだろう。

【0007】

これらの問題は、少なくとも若干の装置が、認証されたソフトウェアの制御の下に動作する、改ざん防止のハードウェアで実行されるのが有利となる場合があるという効果を伴



って、「信頼される」ハードウェアおよびソフトウェア要素の別々の組への復号化用キーへアクセスする、装置のその部分を分離する必要性を提示している。

#### 【0008】

・装置は、メディアストリームを表わすデジタルコンテンツをデコードし、メディアストリームに対する既知の一般再生機能を、これらの機能がデジタルコンテンツの完全な復号化にかかわることなく提供することが、共に可能であることが望ましいだろう。これらの機能は、デジタルコンテンツ内部のナビゲーション（例えば、早送り、および巻き戻しのような機能）、デジタルコンテンツ内部のコンテンツ選択（例えば、チャプタスキップ、およびマルチ-アングル選択などの機能）、あるいは、提示操作（例えば、ストップモーション、コマ送りなどの機能）を含んでいる場合もある。

#### 【0009】

・装置は、そのタイトル、あるいはレーティング、あるいはクリアな状態でその情報を維持するのが概して認容可能な、メディアストリームについての他の情報などのような、1つ以上のメディアストリームについての、メタデータへのアクセスを、これらの機能がデジタルコンテンツの完全な復号化にかかわることなく、提供可能であることが望ましいであろう。

#### 【0010】

・装置は、例えば、同一のメディアストリームについて、ビデオに対するオーディオ、あるいはフランス語バージョンに対する英語バージョン、あるいはイギリスでの公開に対する米国での公開、あるいは「一般公開」バージョンに対する「エアライン」バージョンなどのような、1つ以上のメディアストリームの選択された部分に対しての、異なるエンドユーザへの異なるアクセスを、これらの機能がデジタルコンテンツの完全な復号化にかかわることなく、提供可能であることが望ましいであろう。

#### 【0011】

これらの再生機能、および場合によっては、他のものが、相対的に検証されていないソフトウェアで実行されることは望ましいだろう。1つの実施例では、デジタルコンテンツを復号化するキーへのアクセスは、検証されたハードウェアあるいはソフトウェアだけに認容されることになる。しかしながら、改ざん防止ハードウェア（これは高価であり、さらにアップデートすることが困難であろう）内で実行させることなく、あるいは、検証されたソフトウェア（これも、アップデートするのがさらに困難であり、また、作成がさらに高価となり得る）で実行させることなく、ユーザに利用可能であることが望ましい多くのそのような機能がある。

#### 【0012】

現在、デジタル配布のためのメディアストリームを表わすデジタルコンテンツの符号化に用いられているフォーマット（例えば、MPEG-1、MPEG-2、およびMPEG-4など）は、比較的複雑である。これらのフォーマットでは、デジタルコンテンツは、多数のパケットへ分割される。したがって、メディアストリームのデジタルコンテンツ表示を分析する際は、暗号化は、こうした多くのパケットにわたって、かなりの状態情報を維持することが伴うと予想される。構文解析作業およびステッチ作業の双方を実行可能な装置は、かなりのワーキングメモリを必要とすることになる。一般に、パケットの境界にわたって維持しなければならない状態がより少なくなると、符号化および暗号化された映画を、デコードし、および復号化するハードウェアおよびソフトウェアはより簡単になり、さらに、その映画のためのデジタルコンテンツは、さほどクリアな状態では露出されなくなるだろう。

#### 【0013】

メディアストリームを表わすデジタルコンテンツの符号化に用いられるフォーマットは、デジタルコンテンツの送付が中断され、後に再開される時、あるいはデジタルコンテンツの一部分を含むパケットが順番を狂わせて、あるいは一部分が欠損して到着した時など、そのデジタルコンテンツの一部分を、異なる時間に部分的に配信することにも提供される。多数のパケットに関する問題と同様に、デジタルコンテンツの一部分だけの部分配信

から回復可能な装置は、かなりの状態を維持するか、あるいはかなりのワーキングメモリを維持する必要があるだろう。一般に、パケットの境界にわたって維持しなければならない状態がより少なくなると、符号化され、および暗号化された映画を、デコードし、および復号化するハードウェアおよびソフトウェアは、順序が狂ったり、あるいは一部が欠損して届いたパケットの取扱いに関して、より強健となる。

#### 【0014】

メディアストリームを表わすデジタルコンテンツの符号化に用いられるフォーマットは、メディアストリームが実際にビューアに提示されていないときでさえ、利用可能であることが有利となる、タイトルなどのメディアストリームについての追加情報に提供される。例えば、実際にメディアストリームを提示することなく、潜在的ビューアが、タイトルおよび関連情報をブラウズしたり、あるいはその情報によりコンピュータ化された検索を行うことも可能となるのは有利となろう。そのメディアストリームを表わすデジタルコンテンツに関するランダムアクセスベースなどにおけるように、その情報を迅速に提供し得る装置は、ランダムアクセスベースでレビューされることを所望されるデジタルコンテンツの量に相対的に比例して、こうした装置がこのようにアタックに対して相対的に安全でなくなり、復号化キーあるいはクリアな状態のデジタルコンテンツのいずれかが、こうしたランダムアクセスが所望されるシステムのこれらの部分で利用可能となるという効果を伴って、計算およびメモリのためにかなりのリソースを要することになるだろう。

#### 【0015】

したがって、デジタルコンテンツへアクセス可能な装置も、そのデジタルコンテンツにより表わされるメディアストリームへはアクセスできないが、しかし、そのメディアストリームに関するメタデータへはアクセス可能となる技術など、メディアストリームを表わすデジタルコンテンツの提示のための、改良された技術を提供することは有利となろう。

#### 【課題を解決するための手段】

#### 【0016】

暗号化されたデジタルコンテンツに対応するメディアストリームの安全な提示方法は、以下を含んでいる。(1) メディアストリームを、そのメディアストリームを表わすデジタルコンテンツフォーマットへ符号化すること、(2) メディアストリームを表わすデジタルコンテンツフォーマット全体より少ない、当該デジタルコンテンツの一部分、そのメディアストリームの提示に必要な、暗号化されたデジタルコンテンツの部分を暗号化すること、(3) ここで、デジタルコンテンツの暗号化されたバージョンは、フォーマットパラメータにおいて、そのデジタルコンテンツのクリアなバージョンから実質的に変化していない。

#### 【0017】

メディアストリームを表わすデジタルコンテンツの符号化に使用されるフォーマットは、相対的に高レベルの各層が抽象化を表示し、それに対し、相対的に低レベルの各層がその実現を表わす、階層構造の情報を要約する (encapsulate) ために提供される。本明細書で説明されるように、本発明の1つの態様では、最高レベル層 (あるいは、多数の高レベル層) は、そのメディアストリームに対するオーディオおよびビデオ情報を表わし、一方、相対的に低レベルの層は、その情報が、パケットへ断片化され、索引をつけられ、複合化され、および (例えば、閉じたキャプション化および著作権情報などの) メタデータにより補足される技術を表わしている。本明細書で説明されるように、本発明の1つの態様では、そのメディアストリームに対するオーディオおよびビデオ情報のみが暗号化され、一方、他の相対的に低レベルの層は「クリアな状態」 (すなわち、暗号化されていない) のままとなっている。

#### 【0018】

より一般的に、メディアストリームを表わすデジタルコンテンツの符号化に使用されるフォーマットは、情報が配列されたツリー構造を提供しており、オーディオおよびビデオデータはツリーのリーフに組み入れられ、また、様々なタイプのメタデータ (例えば、制御情報など) はツリーの枝に組み入れられている。本出願を読了の後には、当業者は、ツリ

一構造が唯一可能なフォーマットというわけではなく、一般に、情報のいかなる部分的順序付けであれ、メディアストリームを表わすデジタルコンテンツの符号化に用いるフォーマットにより指定され得ること、ここでは、オーディオあるいはビデオデータが、そのデジタルコンテンツ用のメタデータに関する選択された順序を有するように指定されていることを認めるであろう。

#### 【0019】

本明細書で説明されるように、本発明の1つの態様では、デジタルコンテンツの符号化に用いるフォーマットがツリーとして表示可能であり、それは、暗号化されていないデジタルコンテンツの閉じたルート区画(closed rootward)のサブツリーに十分である。このコンテキストでは、「閉じたルート区画」は、ツリーT内のノードXが1組のノードに含まれている(したがって、暗号化されていない)場合、XからツリーTのルートへ向かう経路内の全てのノードも同様となることを説明している。1つの実施例では、実質的にツリーTの全てのリーフが暗号化され、さらに、システムは、これらのリーフを復号化しなければ、実際のオーディオあるいはビデオを提示できないという唯一の制限を伴って、いまだにMPEGストリームを分析可能である。

#### 【0020】

同様に、デジタルコンテンツの符号化に用いられるそのフォーマットが、部分的順序のとおりに表示可能である場合は、その部分的順序のままそれを暗号化されていないようにするために、その部分的順序の部分の逆方向に閉じれば十分である。このコンテキストでは、「逆方向に閉じる(closed backward)」とは、部分的順序P内の要素Xが1組の要素に含まれている(したがって、暗号化されていない)場合は、部分的順序P内の $Y < X$ となるあらゆる要素Yについても同様であることを説明する。1つの実施例では、部分的順序Pの実質的に全てのオーディオおよびビデオ要素が暗号化されており、さらに、システムは、システムがこれらのオーディオおよびビデオ要素を復号化しなければ、実際のオーディオあるいはビデオを提示できないという唯一の制限を伴って、いまだにMPEGストリームを分析可能である。

#### 【0021】

より一般的に、このコンテキストでは、「暗号化されている」および「暗号化されていない」は、提示装置キーを有することなく、関連要素X、Yをデコードするための異なるレベルの困難さに置き換えてもよい。いかなる形であれ制限を意図するものではない一例をあげると、制御要素、MPEGパケットヘッダー、およびMPEGパックヘッダーが、選択されたパスワードを伴うビットごとのXORなどのように実質的にさほど安全でない技術を用いて暗号化される一方で、ツリーT(あるいは、部分的順序P)のオーディオおよびビデオ要素は、AES-128ブロック暗号を用いて暗号化されていることもあろう。上述したように、さほど強靱でない暗号化された部分が、(ツリーTに対して)閉じたルート区画、あるいは(部分的順序Pに対して)逆方向に閉じているコレクションを形成する限り、システムは、比較的安全ではないハードウェアおよびソフトウェア内でも、MPEGストリームを分析可能であらうし、一方では、オーディオおよびビデオを提示する適切なキーで、比較的安全な部分になお限定されていることになる。

#### 【0022】

本出願の読了後に、当業者は、より一般的に、「暗号化」は、例えば、ROMあるいはASIC内の隠されたマスク層のような物理的ハードウェアセキュリティなどの、いかなるセキュリティ技術でも置き換え可能であると認めるであろう。一例として、セキュリティの多数のレベルは、以下を含むことがあろう。(a) コンピュータ内のファイルのように、読み込み可能な第1レベル；(b) プローブを提示装置の外部ポートと結合することによってのみ読み込み可能である第2レベル、(c) プローブを提示装置の内部バスと結合することによってのみ読み込み可能である第3レベル、(d) 提示装置の回路のエミュレーションによってのみ読み込み可能である第4レベル、および、(e) 集積回路のリバースエンジニアリングおよび電子顕微鏡での検査によってのみ読み込み可能である第5レベル。

## 【0023】

方法の態様は、暗号化のためにデジタルコンテンツのそれらの部分を選択することを含んでいるので、その結果、メディアストリームを表わすデジタルコンテンツの配布においては、例えば以下のような、いかなる実質的な変化もない。(1) デジタルデータの packets 化、あるいは、(2) メディアストリームのオーディオ部分のビデオ部分との同期化。好適な実施例では、変更のない配布は、例えば、MPEG-2 符号化された映画の個々の packets などのように、ビデオ packets データの部分の長さに実質的な変更を加えないことにより、実行可能である。

## 【0024】

1つの実施例では、本方法は、メディアストリームをデジタルコンテンツフォーマット、例えばMPEG-2などに符号化する際、以下を含んでいる。(1) 例えば、packets フォーマット情報のような、ビデオ packets データを説明する情報は、暗号化を控えること、および(2) ブロック換字暗号を使用して、ビデオ packets データを暗号化すること。例えば、ブロック換字暗号は、各 packets 内の16バイトのビデオデータの各シーケンスを、おそらくは、クリアな状態で各 packets 内に15バイトと同数のビデオデータを残す暗号化に用いられる。1つの実施例では、本方法は以下を含んでいる。(3) デジタルコンテンツ内部の、メディアストリームのオーディオ部分、および、おそらくはメディアストリームの他の選択されたデータ部分を別々に暗号化し、メディアストリームのこれらの分離された各データ部分を、異なって選択されたユーザあるいはユーザのグループに対して、異なる形で利用可能にし得るという効果を伴うことになる。

## 【0025】

本発明は映画に限定されず、例えば、アニメーションあるいは音声などの、他のメディアストリームに対しても適用可能であるのみならず、例えば、写真あるいはイラストなどの静止メディアに対しても、さらにデータベースあるいは情報の他のコレクションに対しても適用可能である。

## 【発明を実施するための最良の形態】

## 【0026】

本明細書の説明においては、本発明の好適な実施例は、好適な処理ステップおよびデータ構造を含んで説明されている。本技術分野の技術者ならば、この出願の熟読の後に、本発明の実施例は、過度の実験あるいはさらなる発明を要することなく、明確には説明されていない様々な他の技術を用いて実行され、さらに、こうした他の技術が本発明の範囲および趣旨の中であるであろう。

## 【0027】

## 語彙

これらの以下の各用語の一般的意味は、説明に役立つよう意図されており、決して限定することを意図してはいない。

## 【0028】

・「メディアストリーム」というフレーズは、一連のフレームもしくはフィールドを含む映画、あるいは一連の音声を含むオーディオなど、連続した提示を意図する情報を説明する。本明細書に使用されているように、「メディアストリーム」というフレーズは、(packets を用いて連続送信し、コンテンツ全体が到着する前に再生を始める、音声と画像の)「ストリーミングメディア」の標準的な意味より広い意味を有している。むしろ、本明細書で説明するように、「メディアストリーム」は、連続して届けられなければならないといういかなる特定の要件も存在しない。また、本明細書で説明するように、メディアストリームは、写真あるいはイラストなどのような静止したメディアと同様に、例えば、アニメーションあるいは音声などのような、提示のための他の情報を指す場合もあるし、情報のデータベースおよび他のコレクションを指す場合もある。

## 【0029】

・「デジタルコンテンツ」というフレーズは、エンドビューアへの提示のために、メディアストリームあるいは他の情報を表示することを意図した、デジタルフォーマットのデ

ータを説明する。「デジタルコンテンツ」は、例えば、メッセージヘッダー情報などのパッケージング情報とは区別される。2つのフレーズ「デジタルコンテンツ」および「メディアストリーム」については、前者は後者の選択された符号化を説明しており、後者はその任意の符号化も表示することの結果を説明している。

#### 【0030】

・「メディアストリームに埋め込まれた情報」という語句は、そのメディアストリームを表わす1組のデジタルコンテンツへ、後に検出可能な形式で組み込まれた情報を説明している。例えば、メディアストリームを表わすデジタルコンテンツは、未だに実質的な変化もなくメディアストリームをビューアへ提示可能であるが、そこに埋め込まれた情報は、デジタルコンテンツの適当な処理により回復可能となっているような形で、埋め込まれた情報を含んでいることになろう。

#### 【0031】

・「情報をメディアストリームに埋め込む」というフレーズは、そのメディアストリームを表示し、さらに、後に検出可能な形式で埋め込まれた情報を含む、そのメディアストリームを表わす1組のデジタルコンテンツを生成することを説明する。

#### 【0032】

・「透かし」という用語は、情報をそのデジタルコンテンツに埋め込むことができる、デジタルコンテンツのためのスキーマを説明する。好適な実施例では、関連出願である、2003年1月31日に出願された、米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distribution and Fingerprinting of Digital Content)」(コレンズ (Collens) 他)、および、2003年1月31日に出願された、米国特許出願第10/356,322号「情報の埋め込みに代替ブロックを用いる、デジタルコンテンツの透かし入れおよびフィンガープリンティング (Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information)」(ワトソン (Watson) 他)、において説明されているように、アタッカーは容易には透かしを除去することはできない。しかしながら、本明細書で説明するような透かしの概念は、十分に一般的であるため、アタックに対して抵抗力を持たない透かしも含み得るし、あるいは情報を埋め込むのに他の技術を用いる透かしも含み得る。

#### 【0033】

・「フィンガープリント」という用語、および「埋め込まれた識別情報」というフレーズは、少なくとも1人の指定されたデジタルコンテンツの受取人を識別し得る程度の、情報の特定の組を説明する。好適な実施例では、関連出願である、2003年2月28日に出願された、米国特許出願第10/377,266号「透かしおよびフィンガープリンティングに対する脱同期化アタックからの回復 (Recovery from Desynchronization Attacks against Watermarking and Fingerprinting)」(ワトソン (Watson))、および、2003年2月28日に出願された、米国特許出願第10/378,046号「フィンガープリントされた情報の複数の受取人間の共謀の検出 (Detecting Collusion among Multiple Recipients of Fingerprinted Information)」(ワトソン (Watson))、において説明されているように、共謀した複数のアタッカーは、本発明により提供されるフィンガープリントを容易には取り除くことができず、あるいは、彼らのうちの少なくとも1人がデジタルコンテンツの権限のない配布者として検出されるのを防ぎ得ない。しかしながら、本明細書で説明するようなフィンガープリントの概念は、十分に一般的であるため、取り除きに対してそれほど抵抗力を持たず、もしくは、デジタルコンテンツの権限のない配布者を検出するような能力を提供しないフィンガープリントも含み得る。

#### 【0034】

関連出願である、2003年1月31日に出願された、米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distribution and Fingerprinting of Digital Content)」(コレンズ (Collens) 他)、および、2003年1月31日に出願された、米国特許出願第10/356,322号「情報の埋め込みに代替ブロックを用いる、デジタルコンテンツの透かし入れおよびフィンガープリンティング (Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information)」(ワトソン (Watson) 他)、において説明されているように、「透かし」は、情報が埋め込まれるメディアストリーム内の1組の位置を指し、一方、「フィンガープリント」は、例えば、こうした各位置に対してブロックあるいは代替ブロックを選択するなどにより埋め込まれる、実際の情報を指している。しかしながら、本発明のコンテキストでは、透かしとフィンガープリンティングの概念がこのように制限されなければならない要件は全くない。より一般的には、透かしは、メディアストリーム用のデジタルコンテンツのソースを識別可能ないかなる技術にも使用され得るし、また、フィンガープリントは、メディアストリーム用のデジタルコンテンツの受取人を識別可能ないかなる技術にも使用され得る。例えば、いかなる形であれ制限を意図するものではないが、本明細書で説明したように、情報に透かしを入れること、およびフィンガープリントをほどこすことは、メディアストリームを表わすデジタルコンテンツが、そのソースから送付され、そのエンドビューア (あるいは、それに関連づけられる装置) により受け取られる経路 (あるいは、1組の経路) 全体を表わすことを含んでいる。

#### 【0035】

・「識別情報」という語句は、一般的に、透かしに関連付けられた情報、フィンガープリントに関連付けられた情報、あるいはメディアストリームを表わすデジタルコンテンツの配布が、権限を有しているかいないかを識別し得る情報のいずれかを説明している。

#### 【0036】

・「オリジナルの映画」および「代替映画」というフレーズは、1つは、本発明の態様を用いるシステムへ導入されるそのメディアストリームのオリジナルバージョンであり、そして、他の1つは、オリジナルの映画に応じて生成された、同一メディアストリームの代替バージョンであるといった、同一メディアストリームの代替バージョンを説明する。同様に、「オリジナルブロック」および「代替ブロック」というフレーズは、オリジナルの映画あるいは代替映画内の、同一の個々のブロックあるいはマクロブロックの代替バージョンを説明する。関連出願である、2003年1月31日に出願された、米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distribution and Fingerprinting of Digital Content)」(コレンズ (Collens) 他)、および、2003年1月31日に出願された、米国特許出願第10/356,322号「情報の埋め込みに代替ブロックを用いる、デジタルコンテンツの透かし入れおよびフィンガープリンティング (Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information)」(ワトソン (Watson) 他)、において説明されているように、代替映画は、ほとんどあらゆる点においてオリジナル映画の代わりとなり得るので、オリジナルの映画と代替映画との差は履歴的である。同様に、任意の1つのオリジナルブロックと、その関連する代替ブロックとの差も、代替ブロックが、ほとんどあらゆる点においてオリジナルブロックの代わりとなり得るので、履歴的である。

#### 【0037】

・「オリジナルデジタルコンテンツ」および「変えられたデジタルコンテンツ」(あるいは、後者の場合「ポストアタックデジタルコンテンツ」) という語句は、第1フォーマット (オリジナルデジタルコンテンツ)、および第2フォーマット (変えられたデジタル

コンテンツ)でのメディアストリームを表わすデジタルコンテンツを説明するものであり、変えられたデジタルコンテンツは、オリジナルデジタルコンテンツに対応して、実質的に同様のメディアストリームを表示する意図をもって製作されたものであるが、オリジナルデジタルコンテンツからの識別情報の検出が相対的に困難となるという効果を伴っている。したがって、変えられたデジタルコンテンツは、オリジナルデジタルコンテンツに対する脱同期化アタックの結果である。好適な実施例では、オリジナルデジタルコンテンツは、脱同期化アタックを受ける前の何らかのデジタルコンテンツの実際のオリジナルである場合もあろうし、あるいはオリジナルの映画と代替映画に対応して、もしくは、1組のオリジナルブロックと代替ブロックに対応してデジタルコンテンツの構成された形式である場合もあろう。いかなる方法であれ限定することを意図するものではない一例をあげると、オリジナルデジタルコンテンツは、オリジナルの映画と代替映画との平均である場合もあろうし、あるいは、1つはオリジナルの映画、さらに1つは代替映画という、2組のオリジナルのデジタルコンテンツがある場合もあろう。1つの実施例では、オリジナルデジタルコンテンツの典型的な場合は、オリジナルの映画と代替映画の各ブロックから、ブロックごとの選択を含むことになる。しかしながら、本発明のコンテキストでは、再同期化が探られる「オリジナルデジタルコンテンツ」のように使用され、あるいは含まれるようなフォーマットに対して、特定の制限は存在しない。さらには、以下で説明するように、このテーマの多数の変化は、本発明の範囲と趣旨の中にあり、過度の実験、あるいはさらなる発明を要することなく実行可能であろう。

#### 【0038】

・「エンドビューア」というフレーズは、メディアストリームを表わすデジタルコンテンツのデコードを受け、さらにメディアストリームの提示を受けると考えられる、メディアストリームの受取人を説明する。

#### 【0039】

・「デコード」という用語は、符号化されたフォーマットのメディアストリームを表わすデジタルコンテンツに応じて、メディアストリームの提示の形式でデータを生成することを説明する。本明細書で説明するように、符号化されたフォーマットは、MPEG-2などの業界基準の符号化されたフォーマットを含んでいてもよい。しかしながら、本明細書で説明するようなデコードの概念は、十分に一般的であるため、メディアストリームのための他の符号化フォーマットも含み得る。

#### 【0040】

・「提示 (presentation)」という用語は、例えば、映画を見るためのオーディオおよびビジュアル情報などのような、メディアストリームを見るための形式で情報を生成することを説明する。本明細書で説明するように、映画の提示は、映画のフレームあるいはフィールドのビジュアルディスプレイのみならず、その映画に関連付けられたサウンドトラックのオーディオ提示も含み得る。しかしながら、本明細書で説明するような提示の概念は、十分に一般的であるため、目視される情報の生成のための、他の様々な形式を含み得る。

#### 【0041】

・「パケット」という用語は、例えば、そのデジタルコンテンツ111内部で別々に識別可能である、あるいは、そのデジタルコンテンツを送付する際に送信される、メディアストリームを表わすデジタルコンテンツの一部分を説明する。1つの実施例では、「パケット」は、ピクチャスライスデータを含む、MPEG-2パケットの隣接するサブ領域を示している。本発明のコンテキストでは、「パケット」は、必ずしもMPEG-2パケットと同一というわけではなく、さらに、「パケット」は、必ずしもTCP/IPパケットと同一というわけでもない。

#### 【0042】

これらの用語および概念の拡張を含む本発明の他の、およびさらなるアプリケーションは、この出願を熟読した後には、当業者にとれば明白であろう。これらの他の、およびさらなるアプリケーションは本発明の範囲および趣旨の一部であり、またこれらは、当業者

にとれば、さらなる発明あるいは過度な実験を伴うことなく、明白であろう。

#### 【0043】

本発明の範囲と趣旨は、これらの定義のいずれにも、あるいは、そこで言及された特定の例にも限定されるものではなく、これらのおよび他の用語により実現される最も一般的な概念を含むと意図されている。

#### 【0044】

システムの各要素

図1は、暗号化されたデジタルコンテンツに対応する、メディアストリームの安全な提示のためのシステムのブロック図を示している。

#### 【0045】

システム100は、メディアストリームソース110、配布ネットワーク120、キーサーバ130、および1組の顧客施設装置140を含んでいる。システム100は、1つ以上のメディアストリームを、これらのメディアストリームに関連付けられたデジタルコンテンツにより表示されるものとして、1人以上の特定の選択されたユーザ150へ提示するよう配置されている。

#### 【0046】

メディアストリームソース110は、パケット112のシーケンスの形式で、1組のデジタルコンテンツ111を注入することが可能である。このパケット112のシーケンスは、システム100のユーザ150に対して意図された、少なくとも1つのメディアストリーム用のデジタルコンテンツを含んでいる。1つの実施例では、1つより多いメディアストリームソース110があり得て、そのメディアストリームソース110は、特定の選択されたユーザ150に適したデジタルコンテンツのコピーを注入可能である。

#### 【0047】

配布ネットワーク120は、メディアストリームソース110、キーサーバ130、および顧客施設装置140間で、情報を転送するよう配置されている。1つの実施例では、配布ネットワーク120は、メディアストリームソース110からパケット112を受け取り可能で、これらのパケット112からの情報をキャッシュし、あるいはそうでなければ記憶装置内に維持し、さらに、それらのパケット112に関連付けられたデジタルコンテンツを、特定の選択されたユーザ150へ適合させる、1組の中間キャッシュあるいはソース121を含んでいる。

#### 【0048】

当技術分野の技術者ならば、この出願の熟読の後に、メディアストリームソース110、配布ネットワーク120、および中間キャッシュあるいはソース121を含んでいるシステム100が、関連出願である、2003年1月31日に出願された、米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distribution and Fingerprinting of Digital Content)」(コレンズ (Collens) 他)、および、2003年1月31日に出願された、米国特許出願第10/356,322号「情報の埋め込みに代替ブロックを用いる、デジタルコンテンツの透かし入れおよびフィンガープリンティング (Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information)」(ワトソン (Watson) 他)、において説明されているように、(メディアストリームを表わすデジタルコンテンツの配布に関してさらに説明されるよう) デジタルコンテンツ111を適合させ、暗号化するよう好適に配置されているのを認識するだろう。

#### 【0049】

本明細書でさらに説明されているように、いかなる方法であれ、限定を意図するものではない1つの実施例では、デジタルコンテンツ111は、例えば、関連出願である、2003年1月31日に出願された、米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distrib



ution and Fingerprinting of Digital Content)」（コレンズ (Collens) 他）、および、2003年1月31日に出願された、米国特許出願第10/356,322号「情報の埋め込みに代替ブロックを用いる、デジタルコンテンツの透かし入れおよびフィンガープリンティング (Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information)」、(ワトソン (Watson) 他)、において説明されているように、メディアストリームを表わすそのデジタルコンテンツ111の選択された部分を暗号化され、MPEG-2符号化スキームを用いて符号化されている。そのデジタルコンテンツ111の選択された部分は、メディアストリームの提示可能あるいは表示可能な部分を代表するデジタルコンテンツ111の一部のみを含んでいるのが好ましく、そのメディアストリームを代表する符号化されたデジタルコンテンツ111内に、埋め込まれているときでさえ、いかなるフォーマットデータ、メタデータ、あるいはそのメディアストリームに関連する他の記述データも含まないのが好ましい。

#### 【0050】

本明細書でさらに説明されるように、いかなる方法であれ限定を意図するものではない1つの実施例では、デジタルコンテンツ111のこれらの部分は、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないならば、パケット112のシーケンスが、そのデジタルコンテンツ111に対して生成されたであろう、パケット112のシーケンスをパケット112の代替シーケンスから実質的には変化させないという効果を伴って符号化される。例えば、これは、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないならば、パケット112のシーケンス内の各パケット112長は、そのデジタルコンテンツ111に対して生成されたであろう、パケット112の代替シーケンスから実質的には変化しないという効果を有している。これは、パケット112のシーケンスをデコードするために、したがってそのデジタルコンテンツ111をデコードするために維持される中間状態の量は、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないならば、そのデジタルコンテンツ111に対して生成されたであろう、パケット112の代替シーケンスから実質的には変化しないという効果を有している。

#### 【0051】

本明細書でさらに説明されるように、いかなる方法であれ限定を意図するものではない1つの実施例では、デジタルコンテンツ111のこれらの部分は、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないならば、デジタルコンテンツ111内のオーディオとビデオとの同期化が、そのデジタルコンテンツ111に対して実行されたであろう、そのデジタルコンテンツ111内のオーディオとビデオとの同期化の代替的動作から実質的に変化しないという効果を伴って符号化される。これは、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないならば、そのデジタルコンテンツ111のデコードにかかわる努力の度合いが、オーディオとビデオとの同期化にかかわる、いかなるデコードステップも、そのデジタルコンテンツ111に対して生成されたであろう、そのデジタルコンテンツ111内のオーディオとビデオとの同期化の動作にかかわった努力の度合いと相対的に同等であるという効果を有している。

#### 【0052】

本明細書でさらに説明されるように、いかなる方法であれ限定を意図するものではない1つの実施例では、デジタルコンテンツ111のこれらの部分は、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないならば、デジタルコンテンツ111により表示されるメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シークする」）ことが、そのデジタルコンテンツ111により表示されるメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シークする」）代替動作と実質的に変化しないという効果を伴って符号化される。これは、そのデジタルコンテンツ111がユーザ150への配布のために暗号化されていないなら

ば、デジタルコンテンツ111により表示されるメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シークする」）ことにかかわる努力の度合いが、そのデジタルコンテンツ111に対して実行されたであろう、そのデジタルコンテンツ111により表わされるメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シークする」）代替動作と実質的に変化しないという効果を有している。

#### 【0053】

さらには、本明細書でさらに説明されるように、いかなる方法であれ限定を意図するものではない1つの実施例では、そのデジタルコンテンツ111により表示されるメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シーク」）動作を実行するためにデジタルコンテンツ111の部分を暗号化する必要はない。本出願を読了後は、当業者は、そのデジタルコンテンツ111により表示されるメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シークする」）動作が、相対的に、より効率的に（すなわち、実質的な追加暗号化ステップなしで）、かつ相対的に、より安全に（すなわち、相対的に信頼度の低いハードウェアあるいはソフトウェアコンポーネントにより）実行され得ることを確認するだろう。1つの実施例では、そのデジタルコンテンツ111のMPEG-2の符号化において、そのメディアストリーム内の位置における選択された位置をつきとめる（あるいは、「シークする」）動作に役立つ、デジタルコンテンツ111のこれらの部分は暗号化されない。

#### 【0054】

本明細書でさらに説明されるように、いかなる方法であれ限定を意図するものではない1つの実施例では、デジタルコンテンツ111内で、ビデオブロックデータだけが、好ましくはブロック換字暗号、好ましくはAES-128やAES-256のようなAES暗号の変形形態を用いて暗号化されている。1つの実施例では、ブロック換字暗号は、各パケット112内の16バイトのビデオブロックデータの各シーケンスを暗号化するのに使用可能であるが、暗号化の後、事実、各パケット112内の15バイトと同数のビデオブロックデータが、クリアな状態に留まっているだろう。

#### 【0055】

1つの実施例では、デジタルコンテンツ111は、MPEG「パケット」内に（制御データと同様に）そのオーディオおよびビデオデータを含む、MPEG-2を用いて符号化されている。MPEGパケットは、MPEG「パック」内のMPEG-2により密閉される（*enclosed*）。MPEG規格は、デジタルビデオ産業で既知の文書においてさらに説明されている。こうした実施例では、これは、オーディオデータかビデオデータだけが暗号化されている（しかし、必ずしも全てのオーディオとビデオデータが暗号化されているとは限らない）一方で、（MPEGパケットヘッダー、MPEGパックヘッダー、および一般に全てのタイプのMPEG制御データを含む）実質的に全てのMPEG制御データが暗号化されていないままであるという効果を有している。また、こうした実施例では、これは、MPEGパケットペイロードだけが暗号化されているという効果がある。

#### 【0056】

また、こうした実施例では、MPEGパケットが、暗号化サイズ（16バイト）の整数倍でないペイロードを含んでいるところでは、いかなる残余、場合によれば15バイトと同数も暗号化されずに残っている。これは、こうした実施例では、少なくともいくつかのパケットは、（暗号化されない）パケットヘッダー情報、（暗号化されない）MPEG制御データ、暗号化されたオーディオあるいはビデオデータ、および暗号化されていないままの、おそらく15バイトと同数のオーディオあるいはビデオデータを含み得るという効果を有している。

#### 【0057】

こうした実施例では、MPEGデータが既に他の技術（例えば、MPEGデータを担持する選択されたDVD物理メディアに、使用中であるかもしれないCSSなど）で暗号化されていたなら、他の技術で既に暗号化されたそれらのパケット112は、AES暗号を

用いてさらに暗号化されることはない。当業者は、CSS仕様が、CSSを用いてDVDビデオディスクのセクターの50%以下の暗号化を提供するので、これは、場合によれば、DVDビデオディスクのセクターの50%と同数が、AES暗号を用いて暗号化するために残されているだろうという効果を有することを認めるだろう。

#### 【0058】

こうした実施例では、暗号化されたMPEGパケットのそれらのデータ要素は、MPEGパック情報とMPEGパケット情報へのオフセットとして維持されている。これは、MPEGパック情報とMPEGパケット情報が可変長ヘッダーを有しているが、暗号化されたデータ要素は、これらのヘッダーの終端に対してまだ配置可能であるという効果を有している。

#### 【0059】

本明細書でさらに説明されるように、いかなる方法であれ限定を意図するものではない1つの実施例では、デジタルコンテンツ111内の、例えば、ビデオストリームと区別可能なオーディオストリームなど、分離可能なメディアストリームは、別々に暗号化されるのが好ましく、それにより、分離可能なメディアストリームを、異なる特定の選択されたユーザ150、あるいは特定の選択されたユーザ150の異なるグループに対して、異なる形で利用可能にし得るという効果を伴うことになるだろう。

#### 【0060】

キーサーバ130は、例えば、ユーザ150からの要求に対応するなどして、(公開鍵キー暗号システムで使用されるような対称キーか、非対称暗号キーか、にかかわらず)復号化キー、および特定の選択されたユーザ150に対するライセンス情報を含むデジタル情報を供給することができる。

#### 【0061】

顧客施設装置140は、ローカルライブラリ141、ローカルエリアネットワーク142、および1組のプレーヤー装置143を含んでいる。顧客施設装置140は、パケット112のシーケンス内に含まれるデジタルコンテンツにより表わされるように、特定の選択された顧客施設装置140に関連付けられた、1人以上の特定の選択されたユーザ150へ、1つ以上のメディアストリームを提示するよう配置されている。

#### 【0062】

ローカルライブラリ141は、プロセッサ141a、プログラムおよびデータメモリ、または大容量記憶装置141b、およびフォーマット済メディアリーダー141cを含んでいる。1つの実施例では、ローカルライブラリ141はまた、少なくとも1つの入力要素141d、および少なくとも1つの出力要素141eを含んでいる。メモリまたは大容量記憶装置141bは、本明細書に説明されるようにステップを実行するためのプロセッサ141aにより実行あるいは解釈可能なインストラクション141fを含むことが可能である。メモリまたは大容量記憶装置141bはまた、関連出願である、2003年1月31日に出願された、米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distribution and Fingerprinting of Digital Content)」(コレンズ (Collens) 他)、および、2003年1月31日に出願された、米国特許出願第10/356,322号「情報の埋め込みに代替ブロックを用いる、デジタルコンテンツの透かし入れおよびフィンガープリンティング (Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information)」(ワトソン (Watson) 他)、において説明されているように、おそらくは透かしを入れられた、あるいはフィンガープリントを施された、デジタルコンテンツ111の少なくとも一部分のコピーを維持することが可能である。

#### 【0063】

以下に説明するように、インストラクション141fは、ローカルライブラリ141に以下の動作を実行するよう指示する：

(A 1 a) パケット 1 1 2 のシーケンスのフォーマットを用いて、メディアストリームソース 1 1 0 からデジタルコンテンツ 1 1 1 を受け取る動作、または、

(A 1 b) フォーマット済メディアリーダー 1 4 1 c からデジタルコンテンツ 1 1 1 を受け取る動作；

デジタルコンテンツ 1 1 1 がフォーマット済メディアリーダー 1 4 1 e から受け取られる場合には、そのデジタルコンテンツ 1 1 1 は、以下のようになっていよう。(1) 装置により読み取られる物理メディア上で、既に暗号化されている、(2) 装置により読み取られる物理メディア上で、暗号化されていない、または、(3) 装置により読み取られる物理メディア上で、暗号化されているが、好適でない暗号化技術を用いている。(2) の場合は、いかなるデジタルコンテンツ 1 1 1 も、フォーマット済メディアリーダー 1 4 1 c 以外の装置に移す前に、デジタルコンテンツ 1 1 1 は、フォーマット済メディアリーダー 1 4 1 c、あるいは、それに結合された補助装置により暗号化される。(3) の場合は、いかなるデジタルコンテンツ 1 1 1 も、フォーマット済メディアリーダー 1 4 1 c 以外の装置に移す前に、デジタルコンテンツ 1 1 1 は、好適でない暗号化技術を用いて復号化され、好適な暗号化技術を用いて再暗号化される。

#### 【0064】

(A 2) (任意に) 例えば、デジタルコンテンツ 1 1 1 へのポインタを含むインデックスファイルのような、クリアな状態のそのデジタルコンテンツ 1 1 1 に関連する、少なくとも何らかのメタデータを検索するという効果を伴って、そのデジタルコンテンツ 1 1 1 を部分的にデコードする；

(A 3) その暗号化されたデジタルコンテンツ 1 1 1、および、任意に、そのデジタルコンテンツ 1 1 1 に関連する、少なくとも何らかの復号化されたメタデータをメモリあるいは大容量記憶装置 1 4 1 b に保存する；そして、

(A 4) クリアな状態のそのデジタルコンテンツ 1 1 1 に関するメタデータを検索するという効果、および暗号化された形式で、そのデジタルコンテンツ 1 1 1 により表示されるメディアストリームの提示可能な部分を表示するデータを検索するという効果を伴って、そのデジタルコンテンツ 1 1 1 をデコードする；

(A 5) 暗号化されたデジタルコンテンツ 1 1 1 を、メモリあるいは大容量記憶装置 1 4 1 b から、ローカルネットワーク 1 4 2 およびプレーヤー装置 1 4 3 へ移送する；そして、

(A 6) プレーヤー装置 1 4 3 からの要求に応じて、クリアな状態であるが検出あるいは侵入から安全な、プレーヤー装置 1 4 3 でメディアストリームを表示するためのデジタルコンテンツ 1 1 1 により表示されるデータを検索するという効果を伴って、そのデジタルコンテンツ 1 1 1 の選択された部分を復号化する。

#### 【0065】

適用されるべき特定の技術は、以下でさらに説明する。

#### 【0066】

以下で説明するように、プレーヤー装置 1 4 3 は、以下の動作を実行する：

(B 1) メモリあるいは大容量記憶装置 1 4 1 b、およびローカルネットワーク 1 4 2 からデコードされたデジタルコンテンツ 1 1 1 を受け取る；

(B 2) ユーザ 1 5 0 から 1 組のコマンドあるいはリクエストを受け取る；

(B 3) そのデコードされたデジタルコンテンツ 1 1 1 の暗号化された要素を参照することなく、さらに、そのデコードされたデジタルコンテンツ 1 1 1 に、いかなる復号化も実行することなく実行可能な、ユーザ 1 5 0 からのこれらのコマンドあるいはリクエストを実行する；そして、

(B 4) キーサーバ 1 3 0 からの 1 つ以上の復号化キーを用いて、そのデコードされたデジタルコンテンツ 1 1 1 の要素（オーディオあるいはビデオブロックなど）を復号化することを伴う、デコードされたデジタルコンテンツ 1 1 1 のこれらの要素を示し、あるいは表示する。

#### 【0067】

適用されるべき特定の技術は、以下でさらに説明される。

#### 【0068】

##### 動作方法

図2は、暗号化されたデジタルコンテンツに対応した、メディアストリームの安全な提示のための方法の処理フロー図を示している。

#### 【0069】

順次説明されるが、方法200のフローポイントおよび方法ステップは、結合した、あるいは平行な、別々の要素により、非同期あるいは同期的に、パイプライン化された方法、あるいは他の方法で実行可能である。本発明のコンテキストでは、この方法は、そのように明確に述べられている箇所を除いて、この記述が列挙している、フローポイント、あるいは方法ステップと同一順序で実行されなければならないという、特定の要件は存在しない。

#### 【0070】

フローポイント210では、ローカルライブラリ141は、1つ以上のメディアストリームを表わすデジタルコンテンツ111を受け取る準備ができています。方法200は、ステップ211（メディアストリームソース110からデジタルコンテンツ111を受け取る）、あるいはステップ212（フォーマット済メディアリーダー141cからデジタルコンテンツ111を受け取る）のいずれかを実行する。

#### 【0071】

ステップ211では、ローカルライブラリ141が、メディアストリームソース110から、1つ以上のメディアストリームを表わすデジタルコンテンツ111を受け取る。このステップの一部として、ローカルライブラリ141は、デジタルコンテンツ111をまとめて含む、1つ以上のパケット112のシーケンスを受け取る。このステップの一部として、ローカルライブラリ141は、喪失し、もしくは壊れたパケット112の再送信の要求を必要とされる場合もあり、順序が狂って配信されたパケット112を並べなおすことを必要とされる場合もあり、さらに、既知の区切り点から受信を続けるために、メディアストリームソース110との接続を再び確立することを必要とされる場合もある。このステップの結果として、ローカルライブラリ141は、1つ以上のメディアストリームを表わすデジタルコンテンツ111の少なくとも一部分を取得し、さらに、方法200は、フローポイント220へ進むことが可能である。

#### 【0072】

ステップ212では、ローカルライブラリ141は、フォーマット済メディアリーダー141cから、1つ以上のメディアストリームを表わすデジタルコンテンツ111を受け取る。このステップの一部として、ローカルライブラリ141は、フォーマット済メディアリーダー141cから直接、あるいはそれに結合された補助装置からデータを受け取る。このデータは、ステップ211の実行と同様の方法で、あるいは、例えばDMA転送などのような他の技術により、1つ以上のパケット112のシーケンスで配信され得る。上述したように、このデジタルコンテンツ111は、既に暗号化されているか、暗号化されていないか、あるいは好適でない暗号化技術を用いて暗号化されている。このステップの一部として、上述のように、デジタルコンテンツ111は、結局、フォーマット済メディアリーダー141c以外の任意の装置に移送される以前に、好適な暗号化技術を用いるフォーマットに変換される。このステップの結果として、ローカルライブラリ141は、1つ以上のメディアストリームを表わすデジタルコンテンツ111の少なくとも一部分を取得し、さらに、方法200は、フローポイント220へ進むことが可能である。

#### 【0073】

フローポイント220では、ローカルライブラリ141は、デジタルコンテンツ111を部分的にデコードする準備ができています。このフローポイントに続くステップは、方法200の一部として任意に実行される。

#### 【0074】

ステップ221では、ローカルライブラリ141は、クリアな状態で、そのデジタルコ

コンテンツ 1 1 1に関連する少なくとも何らかのメタデータを得るという効果を伴って、受信したデジタルコンテンツ 1 1 1を部分的にデコードする。1つの実施例では、クリアな状態で得られるメタデータは、デジタルコンテンツ 1 1 1により表示されるメディアストリーム内の選択された位置へのポインタを含む、少なくとも1つのインデックスファイルを含んでいる。方法 2 0 0は、フローポイント 2 3 0へ進むことが可能である。

**【0075】**

フローポイント 2 3 0では、ローカルライブラリ 1 4 1は、メモリあるいは大容量記憶装置 1 4 1 b内にデジタルコンテンツ 1 1 1を保存する準備ができています。

**【0076】**

ステップ 2 3 1では、ローカルライブラリ 1 4 1は、メモリあるいは大容量記憶装置 1 4 1 b内にデジタルコンテンツ 1 1 1を記録する。

**【0077】**

ステップ 2 3 2（フローポイント 2 2 0に続くステップが実行された場合）では、ローカルライブラリ 1 4 1は、デジタルコンテンツ 1 1 1に対応して得られたいかなるメタデータも、メモリあるいは大容量記憶装置 1 4 1 b内に記録する。

**【0078】**

フローポイント 2 3 0に続くステップを実行した結果として、ローカルライブラリ 1 4 1は、暗号化されたデジタルコンテンツ 1 1 1を検索可能であり、さらに任意に、それに関連した、少なくとも何らかの暗号化されていないメタデータが、メモリあるいは大容量記憶装置 1 4 1 bから検索可能である。方法 2 0 0は、フローポイント 2 4 0へ進むことが可能である。

**【0079】**

フローポイント 2 4 0では、ローカルライブラリ 1 4 1は、暗号化されたデジタルコンテンツ 1 1 1をプレーヤー装置 1 4 3に送る準備ができています。

**【0080】**

ステップ 2 4 1では、ローカルライブラリ 1 4 1は、暗号化されたデジタルコンテンツ 1 1 1を検索し、さらに任意に、それに関連する少なくとも何らかの暗号化されていないメタデータを、メモリあるいは大容量記憶装置 1 4 1 bから検索する。

**【0081】**

ステップ 2 4 2では、ローカルライブラリ 1 4 1は、ローカルネットワーク 1 4 2を用いて、暗号化されたデジタルコンテンツ 1 1 1を、メモリあるいは大容量記憶装置 1 4 1 bからプレーヤー装置 1 4 3へ送付する。

**【0082】**

フローポイント 2 4 0に続くステップを実行した結果として、プレーヤー装置 1 4 3は、暗号化されたデジタルコンテンツ 1 1 1へアクセス可能である。方法 2 0 0は、フローポイント 2 5 0へ進むことが可能である。

**【0083】**

フローポイント 2 5 0では、プレーヤー装置 1 4 3は、ユーザ 1 5 0へ暗号化されたデジタルコンテンツ 1 1 1を提示する準備ができています。

**【0084】**

ステップ 2 5 1では、プレーヤー装置 1 4 3は、ローカルネットワーク 1 4 2を用いて、メモリあるいは大容量記憶装置 1 4 1 bから、暗号化されたデジタルコンテンツ 1 1 1を受け取る。

**【0085】**

ステップ 2 5 2では、プレーヤー装置 1 4 3は、ユーザ 1 5 0から1組のコマンドあるいはリクエストを受け取る。

**【0086】**

ステップ 2 5 3では、プレーヤー装置 1 4 3は、そのデコードされたデジタルコンテンツ 1 1 1の暗号化された要素を参照することなく、さらに、そのデコードされたデジタルコンテンツ 1 1 1に、いかなる復号化も実行することなく実行可能な、ユーザ 1 5 0から

のそれらのコマンドあるいはリクエストを実行する。このステップの一部として、プレーヤー装置143は、以下のサブステップの1つ以上を実行することも可能であろう。

**【0087】**

サブステップ253aでは、プレーヤー装置143は、デジタルコンテンツ111内の選択された位置へ、巻き戻しし、早送りし、あるいはそうでなければ「シーク」を行う場合もある。

**【0088】**

サブステップ253bでは、プレーヤー装置143は、デジタルコンテンツ111により表示されるメディアストリームの提示を、一時停止するか、あるいは停止させる場合もある。

**【0089】**

ステップ254では、プレーヤー装置143は、デジタルコンテンツ111により表示されるメディアストリームを実行するために、ユーザ150からのこれらのコマンドあるいはリクエストを実行する。このステップを実行するために、プレーヤー装置143は、以下のサブステップを実行する。

**【0090】**

サブステップ254aでは、プレーヤー装置143は、メディアストリームの提示について説明するメタデータ、およびそのメディアストリームに関連する、実際のオーディオおよびビデオの提示のための暗号化されたデータを得るという効果を伴って、デジタルコンテンツ111をデコードする。

**【0091】**

サブステップ254bでは、プレーヤー装置143は、復号化のための補助装置（あるいは、安全なサブシステム）へ、暗号化されたデジタルコンテンツ111を送付する。

**【0092】**

サブステップ254cでは、復号化の後に、プレーヤー装置143は、補助装置（あるいは、安全なサブシステム）から復号化されたデジタルコンテンツ111を受け取る。

**【0093】**

サブステップ254dでは、プレーヤー装置143は、復号化されたデジタルコンテンツ111に対応してメディアストリームを提示する。

**【0094】**

フローポイント260では、プレーヤー装置143は、ユーザ150からのさらなるコマンドに応じる準備ができており、フローポイント250へ進むことが可能である。

**【0095】****代替的实施例**

本発明は、メディアストリームの配布以外、およびデジタルコンテンツの配布以外のアプリケーションに役立つ、十分な一般性を有している。例えば、本発明は、概して、データセットのセキュリティ、あるいはこれらのデータセットの受取人の識別が望まれているアプリケーションに役立つ。

**【0096】**

本明細書には、好適な実施例が開示されているが、本発明の概念、範囲、および趣旨内に留まりながらも、多くの変形形態が可能である。これらの変形形態は、この出願を熟読すれば、当業者に明白となろう。

**【0097】**

・上述のように、本発明は映画に制限されるものではなく、例えば、アニメーションあるいは音声などの、他のメディアストリームに対しても適切であるのみならず、例えば、写真あるいはイラストなどの静止メディアに対しても、さらにデータベースあるいは情報の他のコレクションに対しても適切なものである。

**【0098】**

この出願を熟読した後は、当業者はこれらの代替的实施例が説明のためのものであり、決して限定するものではないと認めるであろう。

## 【図面の簡単な説明】

【0099】

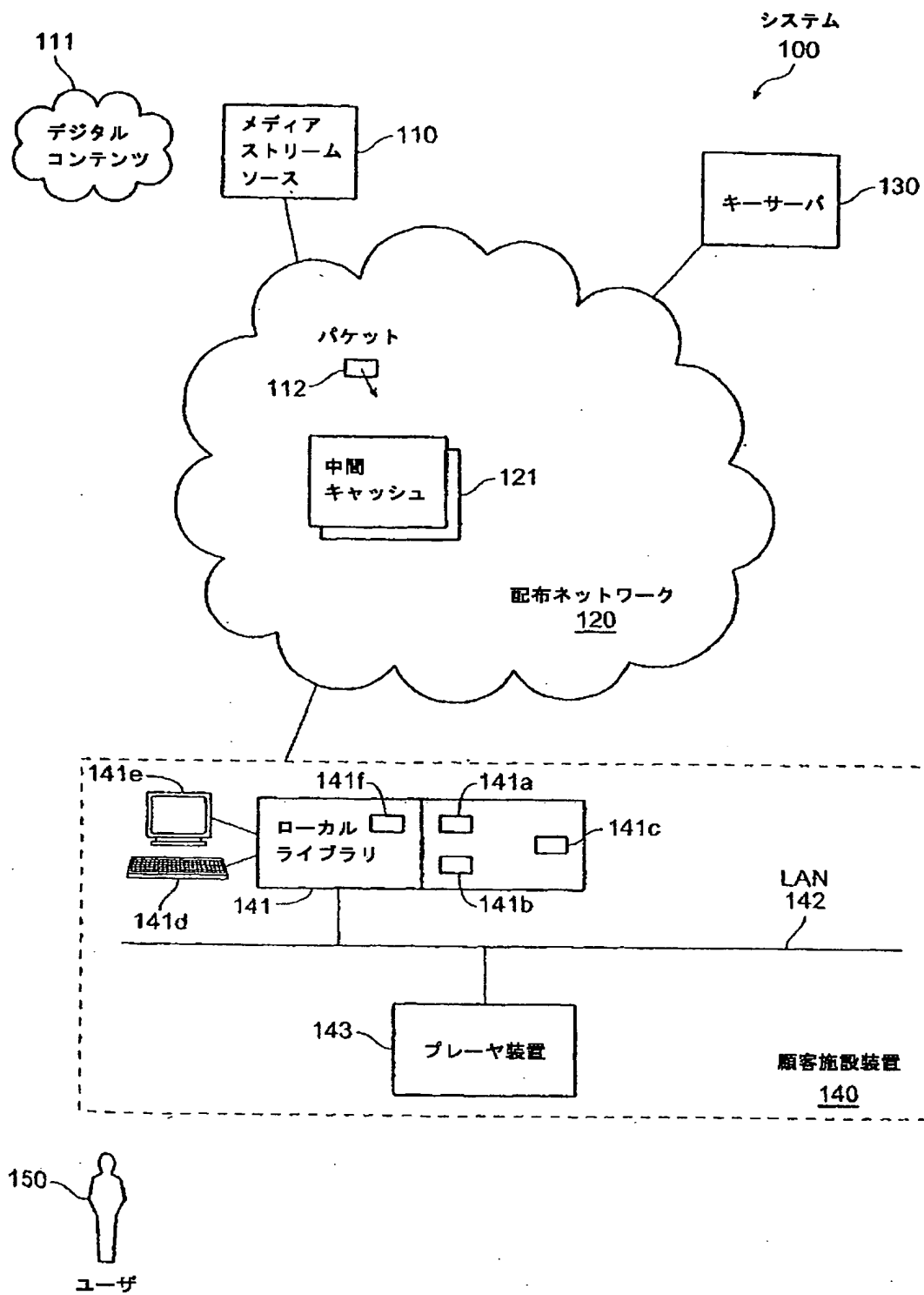
【図1】暗号化されたデジタルコンテンツに対応した、メディアストリームの安全な提示のためのシステムのブロック図である。

【図2】暗号化されたデジタルコンテンツに対応した、メディアストリームの安全な提示のための方法の処理フロー図である。

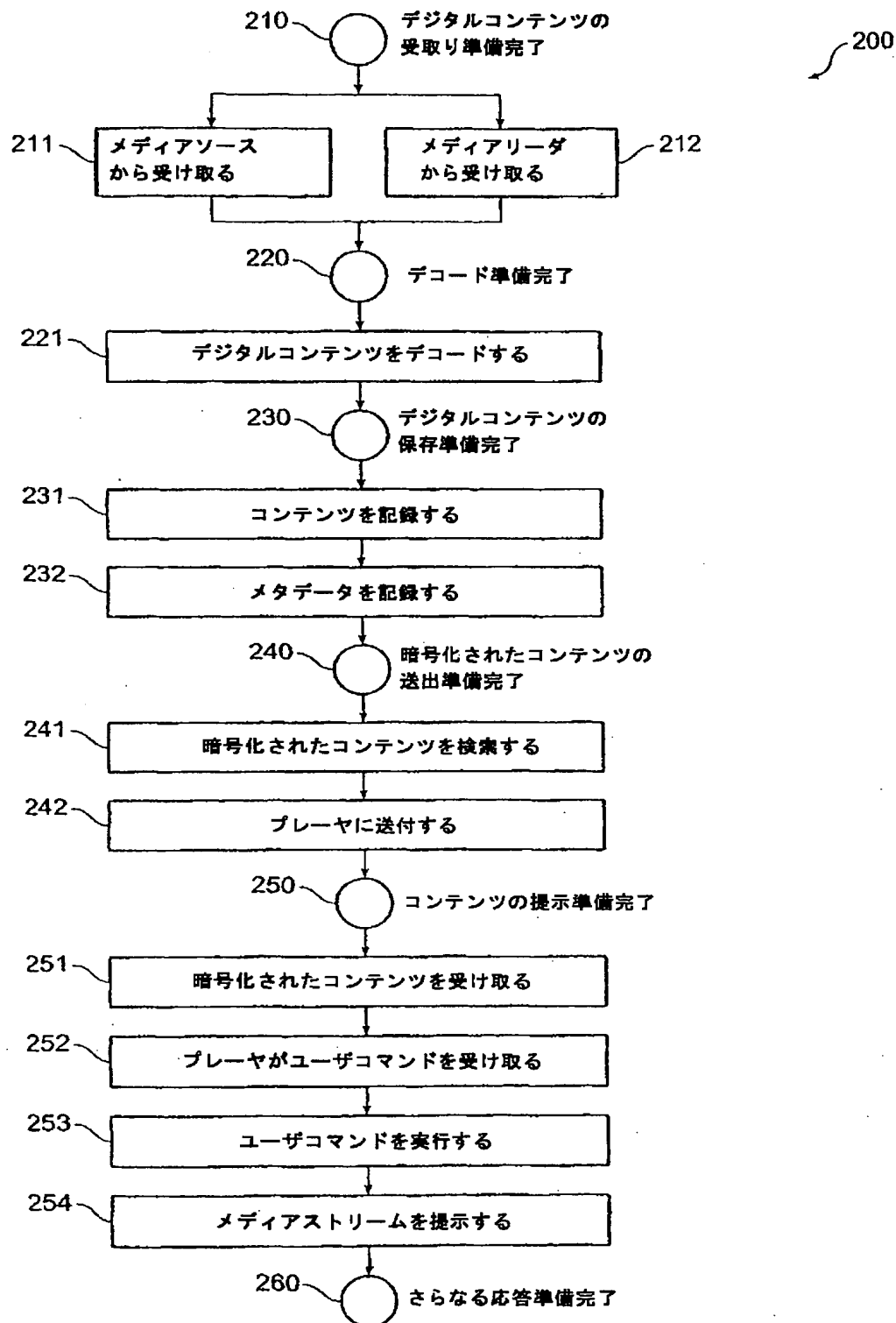


【書類名】図面

【図 1】



【図 2】



## 【書類名】要約書

## 【要約】

メディアストリームの安全な提示(110)は、メディアストリーム(110、111)をデジタルコンテンツ(111)へ符号化し、そのデジタルコンテンツ(230、231、232)の提示に必要な部分を暗号化することを含み、その暗号化されたバージョンは、パラメータのフォーマットにおいて、当該デジタルコンテンツ(111)のクリアなバージョンから、実質的に変化しない。暗号化するためにこれらの部分を選択しても、メディアストリームの配布において全く変化はない: デジタルデータの packets 化、あるいはメディアストリームの音声のビデオ部分との同期化。そのメディアストリームを MPEG-2 へ符号化する際には、ビデオブロックデータを説明する情報、パケットフォーマット情報、ブロック換字暗号を用いる暗号化ビデオブロックデータは、暗号化を控えられる。ブロック換字暗号は、各パケット内の 16 バイトのビデオデータの各シーケンスを、おそらくは、クリアな状態で各パケット内に 15 バイトと同数のビデオデータを残す暗号化に用いられる(260)。